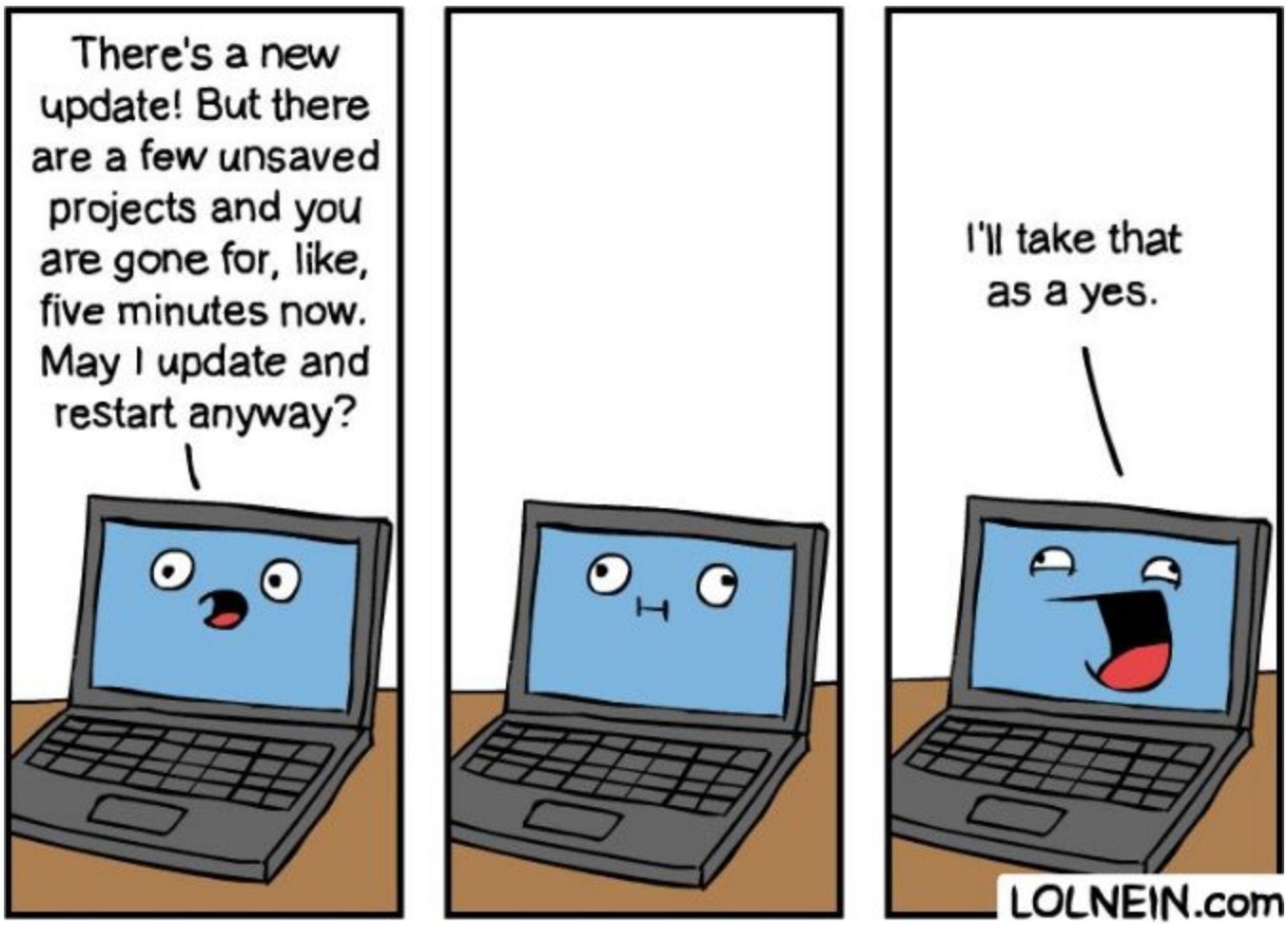
Security Now! #664 - 05-22-18

SpectreNG Revealed

This week on Security Now!

This week we examine the recent flaws discovered in the secure Signal messaging app for desktops, the rise in DNS router hijacking, another seriously flawed consumer router family, Microsoft Spectre patches for Win10's April 2018 feature update, the threat of voice assistant spoofing attacks, the evolving security of HTTP, still more new trouble with GPON routers, Facebook's Android app mistake, BMW's 14 security flaws and some fun miscellany. Then we examine the news of the next-generation of Spectre processor speculation flaws and what they mean for us.

Our Picture of the Week



Security News

Update your Signal Desktop Apps for Windows & Linux
A few weeks ago, Argentinian security researchers discovered a severe vulnerability in the Signal messaging app for Windows and Linux desktops that allows remote attackers to execute malicious code on recipient systems simply by sending a message—without requiring any user interaction.

The vulnerability was accidentally discovered while researchers–amond them Juliano Rizzo–were chatting on Signal messenger and one of them shared a link of a vulnerable site with an XSS payload in its URL. However, the XSS payload unexpectedly got executed on the Signal desktop app!!

(Juliano Rizzo was on the beach when the BEAST and CRIME attacks occurred to him.)

After analyzing the scope of this issue by testing multiple XSS payloads, they found that the vulnerability resides in the function responsible for handling shared links, allowing attackers to inject user-defined HTML/JavaScript code via iFrame, image, video and audio tags.

Using this vulnerability, attackers can even inject a fillable form on the recipient's chat window, tricking them to reveal their sensitive information using social engineering attacks.

Just to be clear: this is not a problem with the Signal protocol design. It's a problem with those specific implementations of Signal.

Interestingly, Signal is another of those apps which was built upon the Electron application platform framework which we discussed as being vulnerable last week.

However, the Open Whisper Systems guys has already addressed the issue and immediately released new versions of Signal app within a few hours of receiving the responsible vulnerability disclosure by the researcher.

Independent of Electron, the primary vulnerability that triggers the code execution has been patched in Signal's stable release version 1.10.1 and pre-release version 1.11.0-beta.3. So Signal users should be sure to update their Signal for desktop applications as soon as possible.

The researchers also found that a patch (regex function to validate URLs) for this vulnerability existed in previous versions of the desktop app, but it was somehow removed or skipped in the Signal update released on 10th April this year.

Since the Signal app has an auto-update mechanism, most users will already have the update installed. But double-checking is worthwhile.

https://support.signal.org/hc/en-us/articles/360003906531-How-do-I-ensure-Signal-Desktop-is-up-to-date-

The latest update also patches a recently disclosed vulnerability in Signal for desktop apps which was exposing disappearing messages in a user-readable database of macOS's Notification Center, even if they are deleted from the app.

The rise in router hijacking is spawning a rise in DNS hijacking
The Hacker News reports:
Widespread routers' DNS hijacking malware that recently found targeting Android devices has now been upgraded its capabilities to target iOS devices as well as desktop users.

Dubbed Roaming Mantis, the malware was initially found hijacking Internet routers last month to distribute Android banking malware designed to steal users' login credentials and the secret code for two-factor authentication.

According to security researchers at Kaspersky Labs, the criminal group behind the Roaming Mantis campaign has broadened their targets by adding phishing attacks for iOS devices, and cryptocurrency mining script for PC users.

So... it is really important to be sure your router's firmware is up-to-date and that its logon credentials are strong.

Anyone who might have a "DrayTek" Router... update your firmware NOW!
DrayTek, a Taiwan manufacturer of broadband routers, switches, firewalls, and VPN devices, announced today that hackers are exploiting a zero-day vulnerability to change DNS settings on some of its routers.

Several users discovered and reported on Twitter that their DrayTek routers had their DNS settings changed and pointing to an unknown server located at 38.134.121.95.

"Notification of Urgent Security Updates to DrayTek routers"
https://www.draytek.com/en/about/news/2018/notification-of-urgent-security-updates-to-draytek-routers
<quote> We have become aware of security reports with DrayTek routers related to the security of web administration when managing DrayTek routers. In some circumstances, it may be possible for an attacker to intercept or create an administration session and change settings on your router. The reports appear to show that DNS settings are being altered. Specific improvements have been identified as necessary to combat this and we are in the process of producing and issuing new firmware. You should install that as soon as possible.

Microcode patches for Win10 / 1803: (last Wednesday)
KB4100347
https://support.microsoft.com/en-us/help/4100347/intel-microcode-updates-for-windows-10-version-1803-and-windows-server

Only for Windows 10 version 1803 and Windows Server version 1803 releases... also known as the April 2018 Update. Earlier versions of Win10 have already received Intel microcode patches via the Windows Update mechanism in KB4090007 and KB4091666.

Spoofing Voice Assistants

(sigh) It was perhaps inevitable. We've had domain name phishing using look-alike domain names. Now we have voice assistant phishing using "sound-alike" trigger phrases!

In a published research paper titled: "Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home" a group of Chinese and US researchers describe their various methods of attacking smart assistants like Amazon Alexa and Google Home.

We've already talked about the problem of applications leaving the microphone "on" and listening in the background, which these guys also describe. But they describe and convincingly demonstrate a more worrisome attack, which they call "voice squatting."

https://sites.google.com/site/voicevpasec/

The idea is to trick the user into opening a malicious app by using voice triggers similar to the ones of authentic apps, and using the malicious apps to either phish users for sensitive data or eavesdrop on their surroundings.

The first of these attacks, "voice squatting", relies upon similarities between the voice commands that trigger specific actions. The researchers registered voice assistant apps (called "skills" by Amazon and "actions" by Google) that trigger on phrases which are deliberately similar to authentic apps.

For example, an attacker can register an app that triggers on the phrase of "open capital won", which is obviously similar to the "open capital one," a command for opening the Capital One home banking app for voice assistants.

This type of attack will not trigger every time but will most likely work for non-native-English speakers who have an accent, or for noisy environments where the command might get misinterpreted.

Similarly, an attacker could also register a malicious app that triggers for "open capital one please," or other variations where the attacker adds words to the trigger, words that are used in common speaking expressions.

In their research they register the attack skill "rap game" which sounds nearly identical to the valid Amazon Echo skill "rat game" and, sure enough, "rap game" wins.

For the Google assistant the registered an attack skill "intraMatic opener" that has similar invocation name with target skill "Entrematic Opener." And, again, when users tried to invoke "Entrematic Opener" the attack skill "intraMatic opener" was invoked instead.

For the extra word attack, they registered an attack skill “rat game please” that adds the additional courtesy "please" to the target skill "rat game" for the Amazon Echo. And they showed that when users attempted to invoke the "rat game" skill by saying "{Alexa}, open rate game please" and specification of the more specifically named skill "rat game please" was invoked instead.

Both Amazon and Google have been notified and have responded... but this is sure to pose a daunting challenge to their voice assistant ecosystems.

The evolution of Web security:
Chrome currently shows a lock icon with a comforting green "Secure" for HTTPS.
Starting this July, Chrome 68 will be showing "Not Secure" for HTTP.
Starting this September, Chrome 69 will remove the "Secure" and show only the lock.

Google has stated that since most traffic is HTTPS anyway, it is no longer necessary to draw the user's attention to the "Secure" indicator. Instead, Chrome will focus on highlighting situations when the user is accessing an insecure HTTP website.

So, in Chrome 70, Google plans to further amplify the "Not Secure" indicator with the addition of an animation that turns the "Not Secure" text to red whenever the user is entering data inside a form on an HTTP site.

Insecure routers -> Botnet -> scan for mining rigs.
About 17 thousand compromised GPON routers, infected with the Satori botnet, are now scanning port 3333 to find publicly exposed Ethereum mining rigs running the Nanopool Claymore Dual Miner software for which a publicly known remote execution vulnerability exists.

Once the attacker identifies an Ethereum miner running the Claymore software they push instructions to reconfigure the device to join the 'dwarfpool' mining pool and use the attacker's Ethereum wallet.

And as for those GPON routers?...
Chinese researchers from 360 Netlab have discovered that one botnet operator has found and is deploying a new zero-day vulnerability affecting those pesky GPON routers. Netlab has not released additional details pending the router's manufacturer's updating. But they have stated that they have been able to reproduce its effects. Netlab wrote: "We tested this payload on two different versions of [South Korean, Dasan] GPON home routers. All work."

The botnet exploiting this new GPON router zero-day is called TheMoon, on old threat that was first spotted in 2014 infecting Linux servers but has more recently been switching to home routers.

"TheMoon" makes it the 6th botnet that's fighting for dominion over GSON routers, worldwide. The others being Hajime, Mettle, Mirai, Muhstik, and Satori, which we discussed last week.

Since GPON stands for "Gigabit Passive Optical Network" this suggests that the routers in question are well connected to the Internet, making them extremely valuable as DDoS attack platforms, scanners, and having a bit beefier processors, perhaps more.

The other botnets are exploiting the first two known vulnerabilities: CVE-2018-10561 and CVE-2018-10562.

Facebook app on Android requests "SuperUser" root-level access.
Whoopsie!
Given Facebook's recent privacy controversies, the timing of this could not have been worse. It was just the result of an innocent coding error in a beta release of the Face app for Android. But the permission dialog which popped up on the screen generated a lot of Twitter traffic and user outrage.

Security researcher looked into what was going on and determined that the package that appeared to be triggering the superuser popup was the "WhiteOps" SDK, a software development kit used for detecting ad fraud and implementing domain white/black-lists.

A Facebook spokesperson subsequently confirmed that the popup dialog was caused by a coding error, saying: "A coding error in one of our anti-fraud systems caused a small number of people running the Facebook app and certain permission management apps on rooted Android phones to see a request for additional access permissions. We do not need or want these permissions, and we have already fixed this issue. We apologize for any confusion."

BMW is scrambling to patch many of its autos back to 2012
The well known TenCent Keen Lab guys spent the year of 2017 poking into the security of BMW autos. And, as a result, BMW is working on firmware updates to fixed 14 flaws which affect high-profile car models including the BMW i series, the X series, and the 3, 5 and 7 series.

Exploitation of the flaws is difficult and requires with a USB connection or access to a GSM cell tower. So the researchers and BMW agreed that the dangers are high-end and do not represent imminent danger to their cars' owners. But they do need to be fixed.

Keen Lab has published a self-redacted paper of their research, but is withholding the exploit details until 2019 to give BMW time to develop and deploy updates.

https://keenlab.tencent.com/en/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

Miscellany

Star Trek continues:
A confirmed second season of "Discovery" and a bunch more Trek movies in development.
https://arstechnica.com/gaming/2018/05/a-dozen-years-after-near-death-star-treks-future-may-be-stronger-than-ever/

SyFy announced the cancellation of "The Expanse" after season three... but Jeff Bezos is a huge fan and he is now in talks to pick up the production and produce, at least, a 4th season.
https://arstechnica.com/gaming/2018/05/has-amazon-stepped-up-to-save-the-expanse-from-cancellation/

Follow-up on the EM-Drive:
It appears that the "thrust" was due to current in the lines supplying the resonant cavity pushing against the Earth's magnetic field. Since, by definition, we cannot take the Earth with us into space -- since leaving the Earth behind is the whole point -- a "space drive" which reduces to a simple magnet and coil is not going to get us there -- or anywhere.
https://arstechnica.com/science/2018/05/nasas-em-drive-is-a-magnetic-wtf-thruster/

SpinRite

Jeff Karpinski in Elizabeth, Colorado
Subject: SpinRite does you know what
Date: 18 May 2018 16:57:50

Hey Steve. Happy SpinRite owner for over a decade. Used it many times on conventional drives but today was a first for me and SSD. My shop PC, which runs CNC for my laser cutter and mill, became sluggish all of a sudden. A peek at the Windows system logs showed an explosion of drive write failure warnings. Promptly rebooted into SpinRite and did a level 1 for a quick assessment. It's only a 250G drive so the scan took just a few minutes - sure enough, some issues in the early sectors. Re-ran SpinRite at level 2 and it took an hour or so to beat through the problem spots. After SpinRite finished "blessing the bits", everything was back to normal. PC performance was back and Windows logs were quiet.

Now my question - if SSD writes are truly randomized across the media as marketing claims, why were the bad sectors on my drive largely contiguous and localized to the beginning of the drive? Also, the SMART window showed no issues being reported whatsoever. Not very "smart" in my book... Im not trusting this drive anymore, so I'll pick up a second drive this weekend and let Windows mirror it.

Thanks as always for a fabulous product and keep up the great work with Security Now! Now that I'm retired, it's the only podcast I listen to.

Cheers, Jeff.

SpectreNG Revealed

Security researchers from Google and Microsoft have found two new variants of the Spectre attack that affects processors made by AMD, ARM, IBM, and Intel.

Everyone is onboard now, including AMD, ARM, IBM, Intel, Microsoft, Red Hat and Ubuntu.

All have security advisories and mitigation advice.

Bug known as SpectreNG

Google and Microsoft researchers independently discovered the bug since many people are now digging deeply into other ways in which processor performance optimizations -- such as speculative execution -- might be leveraged to leak confidential information, especially in any shared hosting environments.

We previously had:
Variant 1: bounds check bypass (CVE-2017-5753) aka Spectre v1
Variant 2: branch target injection (CVE-2017-5715) aka Spectre v2
Variant 3: rogue data cache load (CVE-2017-5754) aka Meltdown

To those we add:
Variant 3a: rogue system register read (CVE-2018-3640)
Variant 4: speculative store bypass (CVE-2018-3639) aka SpectreNG

The Rogue System Register Read is a variation of the Meltdown flaw, whereas Variant 4 is another new attack on speculation... with variant 4 being the most worrisome.

Red hat explains that Variant 4 relies upon the presence of a precisely-defined instruction sequence in the privileged code, as well as the fact that memory read from an address to which a recent memory write has occurred may see an older value and subsequently cause an update into the microprocessor's data cache even for speculatively executed instructions that never actually commit (retire). As a result, an unprivileged attacker could use this flaw to read privileged memory by conducting targeted cache side-channel attacks.

Yesterday, Microsoft wrote:

https://blogs.technet.microsoft.com/srd/2018/05/21/analysis-and-mitigation-of-speculative-store-bypass-cve-2018-3639/

In January, 2018, Microsoft published an advisory and security updates for a new class of hardware vulnerabilities involving speculative execution side channels (known as Spectre and Meltdown). In this blog post, we will provide a technical analysis of an additional subclass of speculative execution side channel vulnerability known as Speculative Store Bypass (SSB) which has been assigned CVE-2018-3639. SSB was independently discovered by Ken Johnson of the Microsoft Security Response Center (MSRC) and Jann Horn (@tehjh) of Google Project Zero (GPZ).

What is affected?
AMD, ARM, and Intel CPUs are affected by CVE-2018-3639 to varying degrees.

What is the risk?
Microsoft currently assesses the risk posed by CVE-2018-3639 to our customers as low. We are not aware of any exploitable instances of this vulnerability class in our software at this time, but we are continuing to investigate and we encourage researchers to find and report any exploitable instances of CVE-2018-3639 as part of our Speculative Execution Side Channel Bounty program. We will adapt our mitigation strategy for CVE-2018-3639 as our understanding of the risk evolves.

What is the mitigation?
Microsoft has already released mitigations as part of our response to Spectre and Meltdown that are applicable to CVE-2018-3639 in certain scenarios, such as reducing timer precision in Microsoft Edge and Internet Explorer. Software developers can address individual instances of CVE-2018-3639 if they are discovered by introducing a speculation barrier instruction as described in Microsoft's C++ developer guidance for speculative execution side channels.

Microsoft is working with CPU manufacturers to assess the availability and readiness of new hardware features that can be used to resolve CVE-2018-3639. In some cases, these features will require a microcode or firmware update to be installed. Microsoft plans to provide a mitigation that leverages the new hardware features in a future Windows update.

Preventing speculation techniques involving SSB

As we've noted in the past, one of the best ways to mitigate a vulnerability is by addressing the issue as close to the root cause as possible. In the case of SSB, there are a few techniques that can be used to prevent speculation techniques that rely on SSB as the speculation primitive.
Speculation barrier via serializing instruction

As with CVE-2017-5753 (Spectre variant 1), it is possible to mitigate SSB by using an instruction which is architecturally defined to serialize execution, thus acting as a speculation barrier. In the case of SSB, a serializing instruction (such as an LFENCE on x86/x64 and SSBB on ARM) can be inserted between the store instruction and the load that could be speculatively executed ahead of the store. For example, inserting an LFENCE on line 2 mitigates the simplified example from this post. Additional information can be found in the C++ Developer Guidance for Speculative Execution Side Channels.

```
01: 88040F      mov [rdi+rcx],al
02: 0FAEE8      lfence
03: 4C0FB6040E  movzx r8,byte [rsi+rcx]
04: 49C1E00C    shl r8,byte 0xc
05: 428B0402    mov eax,[rdx+r8]
```

Speculative store bypass disable (SSBD)

In some cases, CPUs can provide facilities for inhibiting a speculative store bypass from occurring and can therefore offer a categorical mitigation for SSB. AMD, ARM, and Intel have documented new hardware features that can be used by software to accomplish this. Microsoft is working with AMD, ARM, and Intel to assess the availability and readiness of these features. In some cases, these features will require a microcode or firmware update to be installed. Microsoft plans to provide a mitigation that leverages the new hardware features in a future Windows update.
Generally applicable mitigations for SSB

NOTE: Intel has estimated an up to 8% decrease in system performance if this class of possibly-dangerous speculative loading is disabled globally.

There are a number of previously described mitigations that are also generally applicable to SSB. These include mitigations that involve removing sensitive content from memory or removing observation channels. Generally speaking, the mitigation techniques for these two tactics that are effective against CVE-2017-5753 (Spectre variant 1) are also applicable to SSB.

Also... Jann Horn at Google, who was the original discoverer of the Meltdown and Spectre flaws has also published proof-of-concept code:
https://bugs.chromium.org/p/project-zero/issues/detail?id=1528

Hi!

After Michael Schwarz made some interesting observations, we started looking into variants other than the three already-known ones.

I noticed that Intel's Optimization Manual says in section 2.4.4.5 ("Memory Disambiguation"):

A load instruction micro-op may depend on a preceding store. Many microarchitectures block loads until all preceding store address are known.

The memory disambiguator predicts which loads will not depend on any previous stores. When the disambiguator predicts that a load does not have such a dependency, the load takes its data from the L1 data cache.

Eventually, the prediction is verified. If an actual conflict is detected, the load and all succeeding instructions are re-executed.

According to my experiments, this effect can be used to cause speculative execution to continue far enough to execute a Spectre-style gadget on a pointer read from a memory slot to which a store has been speculatively ignored.

Intel has announced new patches.

We've already delivered the microcode update for Variant 4 in beta form to OEM system manufacturers and system software vendors, and we expect it will be released into production BIOS and software updates over the coming weeks. This mitigation will be set to off-by-default, providing customers the choice of whether to enable it. We expect most industry software partners will likewise use the default-off option. In this configuration, we have observed no performance impact. If enabled, we've observed a performance impact of approximately 2 to 8 percent based on overall scores for benchmarks like SYSmark® 2014 SE and SPEC integer rate on client1 and server2 test systems.

This same update also includes microcode that addresses Variant 3a (Rogue System Register Read), which was previously documented publicly by Arm* in January. We have not observed any meaningful performance impact on client or server benchmarks with the Variant 3a mitigation.3 We've bundled these two microcode updates together to streamline the process for our industry partners and customers. This is something you will see us continue, as we recognize that a more predictable and consolidated update process will be helpful to the entire ecosystem.